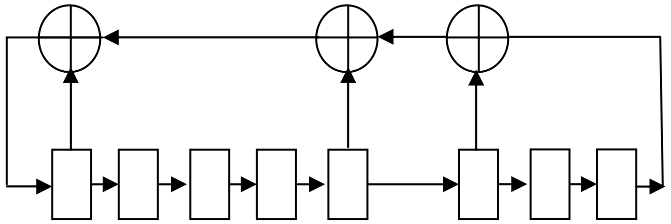
COE 205, Term 033

Computer Organization & Assembly Programming
Programming Assignment# 4

Due date: Saturday, August 7, 2004

You are required to write an 8086 assembly program to implement a pseudo random generator using Liner Feedback Shift Register (LFSR). An example of an 8-bit LFSR is shown below:



Two important characteristics of an LFSR are the Feedback Polynomial, which determines the FFs that are XORed to compute the shifted bit, and the seed which determines the initial content of the FFs. Depending on the Feedback polynomial, the LFSR can generate a maximal-length sequence without repetition, or it may not. The seed can be any number other than 0.
The 8-bit LFSR shown above is a maximal-length i.e. it is guaranteed to generate a random sequence in the range from 1 to 255 before it repeats again.
The Feedback polynomial for the above LFSR can be represented as 10001101. Note that 1 indicates that there is feedback connection, while 0 indicates that there is no feedback connection.

(i) Write a procedure, RAND8, that implements an 8-bit pseudo random generator. The procedure should be given the Feedback polynomial, and the seed, and it should generate the next random number. Assume that the Feedback polynomial and the seed are passed on the stack such that the Feedback polynoimal is pushed first followed by the seed. Assume also that the generated number will be returned on the stack in the same place of the Feedback polynomial while the seed position is freed.

(ii) Write a macro that displays the content of an 8-bit register in decimal.

(iii) Using the procedure and macro in (i) and (ii), generate the first 256 random numbers that will be obtained from the feedabck polynomial 10001101 and an initial seed of 00000001. Determine that it generates 255 different numbers before it repeats.

(iv) Using the procedure and macro in (i) and (ii), generate the first 256 random numbers that will be obtained from the feedabck polynomial 10001101 and an initial seed of 1010101. Determine that it generates 255 different numbers before it repeats.

(v) Using the procedure and macro in (i) and (ii), generate the first 256 random numbers that will be obtained from the feedabck polynomial 10000001 and an initial seed of 00000001. Determine if this feedback polynomial is maximal sequence or not. Justify your answer.

(vi) Ask the user to enter a feedback ploynomial and a seed. Then, ask the user to enter a string of characters. Then, encrypt the string using RAND8 as follows. Each character is encrypted by XORing the least significant 4-bits of the ASCII code of the character with the lest significant 4 bits of the generated random number. For example, assume the character to be encrypted is A=41H and the random number is AAH. Then, the encrypted character will have the ASCII code 4BH = K. To decrypt the character, the decrypted character 4BH=character K, will be XORed with the same corresponding random number used for encryption i.e. AA and this will generate the original character 41H= character A. As an example show the encryption of the string Hello COE-205!!. Then, rerun your program giving it the encrypted string and it should correctly decrypt it to Hello COE-205!!. Try this with the feedback polynomial 10001101 and a seed of 10101010.

Make sure that your program is well documented. Provide a hard copy of the program and a soft copy of both the assembly code and the executable stored in a floppy disk.